ABSTRACT OF THE DISCLOSURE

A data authentication system that at the sender produces for a plurality of data packets a plurality of "integrity checks" by selecting an integrity function from a family or set of integrity functions, selecting a number of bytes from a given packet and manipulating the bytes in accordance with the selected integrity function to produce the integrity check. The system then selects corresponding bytes or bytes that are offset from the corresponding bytes from a next packet and produces a next associated integrity check using the same or another selected integrity check function, and so forth. The system encrypts the integrity checks associated with the plurality of data packets using, for example, a shared secret key, and produces an integrity block. The system then sends the encrypted integrity block and the data packets to the intended recipients. A recipient decrypts the integrity block using the shared secret key and reproduces the integrity checks. It then uses the integrity checks to authenticate the associated data packets by manipulating selected data bytes in accordance with selected integrity check functions. The recipient thus authenticates a plurality of data packets by performing a single decryption operation and a plurality of relatively fast integrity check operations using a selection of integrity check functions that are unknown to an interloper. The sender may also include in a transmission one or more extraneous, or "chaff," data packets, which are data packets that intentionally fail the associated integrity checks. The sender may, for example, include in a transmission multiple sets of packets with the same sequence numbers. The recipient readily determines which of the packets with the same sequence numbers are valid using the appropriate integrity check. However, an interloper who cannot decipher the encrypted integrity block cannot as easily determine which of the packets are valid, and thus, cannot determine which packets to alter and/or how to alter these packets without detection by the integrity checks.